### > ALCUNI SUGGERIMENTI PER EVITARE I VIRUS

1 Installare un antivirus di nota funzionalità (AVG Antivirus, eTrust, McAfee, Panda Software, Symantec, TrendMicro). Meglio aggiungere una anti Firewalls per le intrusioni dall'esterno di hackers o cavalli di troia.

2 Aggiornare quotidianamente il proprio antivirus attraverso aggiornamenti manuali o automatici.

3 Non aprire allegati e/o messaggi che provengono da persone sconosciute. Spesso l'oggetto ed il corpo di un messaggio contiene frasi vaghe, sospette, frasi in inglese, testo ed oggetto completamente diversi tra loro.

4 Evitare il salvataggio e/o esecuzione automatica di files allegati ai messaggi.

5 Controllate i files allegati prima di aprirli. Spesso i files infetti hanno l'estensione **.pif** (estensione che identifica i files che forniscono informazioni a Windows per l'esecuzione di programmi DOS).


Non trattandosi di documenti è molto improbabile che qualcuno vi mandi dei files di questo tipo. Altro esempio di file allegato infetto è quello di un file con doppia estensione (ad esempio **nomefile.txt.pif** o **nomefile.doc.pif**). Se avete dei dubbi è più conveniente NON APRIRE files sospetti. Ricordarsi che i virus confidano nella curiosità delle persone per essere aperti e così attivati, pertanto, la curiosità è la prima nemica.


Diffidare, anche se provenienti da indirizzi conosciuti, dei messaggi che hanno come files allegati degli aggiornamenti a programmi e/o delle protezione contro i virus. Nelle settimane scorse è arrivato un virus proveniente dal falso indirizzo support@microsoft.com che prometteva un aggiornamento per Windows e chi l'ha aperto è stato infettato.

**I links interessanti:**
www.grisoft.com
www.my-etrust.com
www.mcafee.com
www.pandasoftware.com
www.symantec.com
www.trendmicro.com

Per ulteriori informazioni e/o contribuiti a migliorare
le suddette indicazioni, scrivetemi:
lorenzotomassoli@coordinamentocamperisti.it
www.lorenzotomassoli.it